Several Classes of Concatenated Quantum Codes: Constructions and Bounds*

Hachiro FUJITA†

Abstract

In this paper we present several classes of asymptotically good concatenated quantum codes and derive lower bounds on the minimum distance and rate of the codes. We compare these bounds with the best-known bound of Ashikhmin–Litsyn–Tsfasman and Matsumoto. We also give a polynomial-time decoding algorithm for the codes that can decode up to one fourth of the lower bound on the minimum distance of the codes.

1 Introduction

Quantum error correction is a basic technique for transmitting quantum information reliably over a noisy quantum channel. Many explicit constructions of quantum error-correcting codes have been proposed so far. Some of the best-known code constructions are the CSS code construction of Calderbank and Shor [4] and Steane [24] and the stabilizer code construction of Gottesman [13, 14] and Calderbank *et al.* [2, 3]. CSS codes are constructed by using classical error-correcting codes and have a simple decoding algorithm. On the other hand, stabilizer codes are the most general class of quantum error-correcting codes known to date and can be understood by using a theory of additive codes over GF(4), the Galois field with four elements.

As in classical coding theory, we want to construct quantum codes with large minimum distance. More generally, we want to construct asymptotically good quantum codes that have minimum distance proportional to the code length. Ashikhmin *et al.* [1] and Chen *et al.* [6] constructed asymptotically good quantum codes based on algebraic geometry codes. Later, Matsumoto [22] improved the bound of Ashikhmin *et al.* [1].

In classical coding theory, code concatenation [10] is a basic method for constructing good error-correcting codes and most of the known asymptotically good binary codes are constructed by code concatenation [8]. In 1971,

*This paper was presented in part at the IEICE Technical Meeting on Information Theory, Nagoya, Japan, March 2006.

†Superrobust Computation Project, University of Tokyo, 5-1-5 Kashiwanoha, Kashiwa-shi, Chiba 277-8561, Japan. E-mail: fujita@it.k.u-tokyo.ac.jp

Zyablov [25] constructed a family of asymptotically good binary codes by concatenating Reed–Solomon (RS) outer codes with good binary inner codes, and obtained the bound on the minimum distance of the codes, which is called the Zyablov bound.

In the quantum setting, code concatenation is also effectively used to construct good quantum error-correcting codes, although concatenation is mainly used for fault-tolerant quantum computation [20]. Gottesman states code concatenation in his PhD thesis and gives the stabilizer of a quantum code constructed by concatenating the five-qubit code with itself. Calderbank *et al.* [3] also remark concatenated codes and Rains [23] proves the so-called product bound of concatenated codes.

In this paper we present several classes of concatenated quantum codes, more specifically quantum analogues of the Zyablov codes, generalized concatenated codes, and the Blokh–Zyablov codes, and give the bounds on the minimum distance of these codes. We also give a quantum analogue of the Katsman–Tsfasman–Vlăduţ bound based on algebraic geometry codes.

This paper is organized as follows: In Section 2, we review stabilizer codes and the concept of code concatenation, give a quantum analogue of the Zyablov codes, which is constructed by concatenating quantum Reed–Solomon outer codes [15] with good stabilizer inner codes, and derive a lower bound on the minimum distance of the codes. In Section 3, we extend the quantum Zyablov codes to the quantum version of generalized concatenated codes and improve the quantum Zyablov bound. Furthermore, we give a quantum analogue of the Blokh–Zyablov bound. In Section 4, we present a class of concatenated quantum codes based on algebraic geometry codes and give a quantum analogue of the Katsman–Tsfasman–Vlăduţ bound. In Section 5, we discuss the decoding of the concatenated quantum codes constructed in this paper. Based on the result of Hamada [16], we can show that the quantum Zyablov codes achieve the capacity attainable by general stabilizer codes in time polynomial in block length. This coding scheme should be contrasted with the random stabilizer coding scheme which requires exponential time complexity to achieve the same capacity, although the error exponent of the general stabilizer codes is much better that that of the quantum Zyablov codes. In Section 6, we give the conclusion of the paper.

2 Code concatenation and the quantum Zyablov bound

We denote the finite field (Galois field) with q elements by $\mathbb{F}_q$ (not by $\mathrm{GF}(q)$), where q is a prime power, and the q-ary entropy function by

$$H_q(x) = -x \log_q \frac{x}{q-1} - (1-x) \log_q (1-x), \quad 0 < x < 1.$$

If $q = 2$, then $H_2(x)$ is the binary entropy function and denoted by $H(x)$ for simplicity. Following the line of Calderbank *et al.* [3], we explain stabilizer quan-

tum codes (quantum codes for short) and the construction of the concatenated quantum codes. We also give the quantum Gilbert–Varshamov bound for the general stabilizer quantum codes. Stabilizer quantum codes can be related with self-orthogonal additive codes over $\mathbb{F}_4$. Let ω be a primitive element of $\mathbb{F}_4$ that satisfies $\omega^2 = \omega + 1$. Then $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$. We define conjugation by $\bar{x} := x^2$ for $x \in \mathbb{F}_4$. Let $\boldsymbol{u} = (u_1, u_2, \cdots, u_n)$, $\boldsymbol{v} = (v_1, v_2, \cdots, v_n) \in \mathbb{F}_4^n$. We define the trace inner product of $\boldsymbol{u}$ and $\boldsymbol{v}$ as:

$$\langle \boldsymbol{u}, \boldsymbol{v} \rangle := \sum_{i=1}^{n} (u_i \overline{v_i} + \overline{u_i} v_i).$$

A classical *additive* code over $\mathbb{F}_4$ of length n is an additive subgroup of $\mathbb{F}_4^n$. If C is an $(n, 2^{n-k})$ additive code, its *trace-dual* (simply *dual*) of C is defined to be

$$C^{\perp} := \{\boldsymbol{u} \in \mathbb{F}_4^n \mid \langle \boldsymbol{u}, \boldsymbol{v} \rangle = 0 \text{ for all } \boldsymbol{v} \in C\}.$$

Then $C^{\perp}$ is an $(n, 2^{n+k})$ additive code. If $C \subseteq C^{\perp}$, then C is said to be *self-orthogonal*. For $\boldsymbol{u} \in \mathbb{F}_4^n$, we define the *weight* of $\boldsymbol{u}$ to be the number of nonzero components of $\boldsymbol{u}$. Let C be an $(n, 2^{n-k})$ self-orthogonal additive code. Then the codes $C \subseteq C^{\perp}$ correspond to a quantum code Q that encodes k qubits in n qubits. If there are no vectors of weight $< d$ in $C^{\perp} \setminus C$, then Q can correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors [3, Theorem 2] and d is called the *minimum distance* of Q. We denote by $[[n, k, d]]$ the parameters of such a quantum code Q. Let $R_Q := k/n$ and $\delta_Q := d/n$.

Theorem 2.1 ([9, 2]). *For all sufficiently large n, there exists an $[[n, k, d]]$ quantum code satisfying*

$$R_Q \geq 1 - 2H_4(\delta_Q) = 1 - \delta_Q \log_2 3 - H(\delta_Q). \tag{1}$$

Eq. (1) is called the *quantum Gilbert–Varshamov* (GV) bound, since this bound is a quantum analogue of the GV bound for classical binary (not necessarily linear) codes. For self-containedness, we give a proof of Theorem 2.1 in Appendix A. The proof of Theorem 2.1 is not constructive and it requires exponential time complexity to find a quantum code satisfying Eq. (1). Later, we compare this nonconstructive bound with our constructive ones. We are now ready to introduce concatenated quantum codes [14, 3].

Theorem 2.2 ([3]). *If Q_1 is an $[[n_1 m, k]]$ quantum code such that the associated $(nm, 2^{nm+k})$ code has minimum nonzero weight d_1 considered as a block code over an alphabet of size 4^m, and Q_2 is an $[[n_2, m, d_2]]$ quantum code, then encoding each block of Q_1 using Q_2 produces an $[[n = n_1 n_2, k, d \geq d_1 d_2]]$ concatenated quantum code.*

The proof of the above theorem will be clear from the construction of quantum Zyablov codes below. A clear explanation of concatenated quantum codes can be found in [17, Sect. IV]. To construct quantum Zyablov codes, we need quantum Reed–Solomon codes introduced by Grassl *et al.* [15]. Let m be a

positive integer. A classical *Reed–Solomon* (RS) code $C_{\rm RS}$ of length $n = 2^m - 1$ over $\mathbb{F}_{2^m}$ is a cyclic code with generator polynomial

$$g(x) = \prod_{i=0}^{d-2} \left(x - \alpha^i\right),$$

where α is a primitive element of $\mathbb{F}_{2^m}$ and $2 \leq d \leq 2^m - 1$. $C_{\rm RS}$ has dimension $k = n - d + 1$ and minimum distance d. RS codes are nonbinary codes. We need a binary expansion of $C_{\rm RS}$.

Definition 2.3. Let C be a linear code of length n over $\mathbb{F}_{2^m}$, and let $\mathcal{B} = \{b_1, \ldots, b_m\}$ be a basis of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$. Then the *binary expansion* of C with respect to the basis $\mathcal{B}$, denoted by $\mathcal{B}(C)$, is the binary linear code of length nm given by

$$\mathcal{B}(C) := \left\{ (c_{ij})_{i,j} \in \mathbb{F}_2^{nm} \;\middle|\; \boldsymbol{c} = \left(\sum_{j=1}^{m} c_{ij} b_j \right)_i \in C \right\}.$$

For $k \leq 2^{m-1} - 1$, the RS code $C_{\rm RS}$ is self-orthogonal with respect to the standard inner product of $\mathbb{F}_{2^m}$ [15, Lemma 2] and so is the binary expansion $\mathcal{B}(C_{\rm RS})$ of $C_{\rm RS}$ with respect to a self-dual basis $\mathcal{B}$ [15, Corollary 1]. Using the binary expansion of the RS code $C_{\rm RS}$ over $\mathbb{F}_{2^m}$ with parameters $[n, k, d]$, where $k \leq 2^{m-1} - 1$, with respect to a self-dual basis $\mathcal{B}$, one can construct a $[[mn, m(n-2k)]]$ stabilizer quantum code $Q_{\rm RS}$ with associated additive codes $C = \omega\mathcal{B}(C_{\rm RS}) + \bar{\omega}\mathcal{B}(C_{\rm RS})$ and $C^\perp = \omega\mathcal{B}(C_{\rm RS}^\perp) + \bar{\omega}\mathcal{B}(C_{\rm RS}^\perp)$ with parameters $(nm, 2^{nm-m(n-2k)})$ and $(nm, 2^{nm+m(n-2k)})$, respectively (see [3, Theorem 9]). We call $Q_{\rm RS}$ a *quantum Reed–Solomon* (RS) code. $Q_{\rm RS}$ has minimum distance at least $k + 1$. Although we describe quantum RS codes in terms of additive codes over $\mathbb{F}_4$, quantum RS codes are a class of CSS codes [15].

We now give the detail of the construction of concatenated quantum codes based on quantum RS codes. Let $Q_1 = Q_{\rm RS}$ be an $[[nm, m(n-2k)]]$ quantum RS code with associated codes C_1, $C_1^\perp$ with parameters $(nm, 2^{nm-m(n-2k)})$, $(nm, 2^{nm+m(n-2k)})$ as above, where $k \leq 2^{m-1} - 1$. Then the associated code $C_1^\perp$ has minimum nonzero weight $k + 1$ considered as a block code over an alphabet of size 4^m. Let Q_2 be an $[[n_2, m, \delta_2 n_2]]$ quantum code with associated additive codes C_2, $C_2^\perp$ with parameters $(n_2, 2^{n_2 - m})$, $(n_2, 2^{n_2+m})$ and suppose that Q_2 meets the quantum GV bound (1):

$$\delta_2 = H_4^{-1}\left(\frac{1-r}{2}\right), \tag{2}$$

where $r = m/n_2$. Since $C_2^\perp/C_2$ has a natural symplectic structure, there exists an inner-product-preserving map ρ from $\mathbb{F}_4^m$ to $C_2^\perp/C_2$, i.e., each $\boldsymbol{v} \in \mathbb{F}_4^m$ in 1-1 corresponds to $\rho(\boldsymbol{v}) \in C_2^\perp/C_2$ (see Appendix B). We also denote by $\rho(\boldsymbol{v})$ a representative of the coset $\rho(\boldsymbol{v})$. We define additive codes $\rho(C_1)$, $\rho(C_1^\perp)$ as

$$\begin{aligned}\rho(C_1) &:= \{(\rho(\boldsymbol{v}_1)+\boldsymbol{u}_1, \rho(\boldsymbol{v}_2)+\boldsymbol{u}_2, \ldots, \rho(\boldsymbol{v}_n)+\boldsymbol{u}_n) \mid \\ &\qquad (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n) \in C_1, \boldsymbol{u}_i \in C_2, 1 \le i \le n\}, \\ \rho(C_1^{\perp}) &:= \{(\rho(\boldsymbol{v}_1)+\boldsymbol{u}_1, \rho(\boldsymbol{v}_2)+\boldsymbol{u}_2, \ldots, \rho(\boldsymbol{v}_n)+\boldsymbol{u}_n) \mid \\ &\qquad (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n) \in C_1^{\perp}, \boldsymbol{u}_i \in C_2, 1 \le i \le n\}.\end{aligned}$$

Then it is easy to see that $\rho(C_1)$ and $\rho(C_1^{\perp})$ have parameters $(nn_2, 2^{nn_2-m(n-2k)})$ and $(nn_2, 2^{nn_2+m(n-2k)})$, respectively, and that $\rho(C_1)^{\perp} = \rho(C_1^{\perp})$. The resulting quantum code Q with associated codes $\rho(C_1)$, $\rho(C_1^{\perp})$, called a *quantum Zyablov* code, has rate $R = r(1-2r')$, where $r' = k/n$, $0 < r' < 1/2$.

Lemma 2.4. *Let δ be the relative minimum distance of Q. Then $\delta \ge \delta_2 r' = r' H_4^{-1}\left(\frac{1-r}{2}\right)$.*

Proof. Let $\boldsymbol{c} = (\rho(\boldsymbol{v}_1)+\boldsymbol{u}_1, \ldots, \rho(\boldsymbol{v}_n)+\boldsymbol{u}_n) \in \rho(C_1^{\perp}) \backslash \rho(C_1)$, where $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n) \in C_1^{\perp}$ and $\boldsymbol{u}_i \in C_2, 1 \le i \le n$. If $\boldsymbol{v}_i = \boldsymbol{0}$ for all i, then $\rho(\boldsymbol{v}_i)+\boldsymbol{u}_i \in C_2$ for all i and hence $\boldsymbol{c} \in C_2 \oplus \cdots \oplus C_2 \subseteq \rho(C_1)$, which is a contradiction. Hence $(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n)$ is a nonzero codeword of $C_1^{\perp}$ and has at least $k+1$ nonzero components. For each nonzero component $\boldsymbol{v}_i$, $\rho(\boldsymbol{v}_i)+\boldsymbol{u}_i \in C_2^{\perp} \setminus C_2$ has weight at least $\delta_2 n_2$ and hence $\boldsymbol{c}$ has weight at least $\delta_2 n_2 (k+1)$. This shows that the minimum distance of Q is at least $\delta_2 n_2 (k+1)$. From Eq. (2) the statement follows. □

For any given R, $0 < R < 1$, we maximize the relative minimum distance δ of Q under the condition $R = r(1-2r')$. From the above lemma we have

$$\delta \ge \max_{R<r<1} \frac{1}{2}\left(1 - \frac{R}{r}\right) H_4^{-1}\left(\frac{1-r}{2}\right). \tag{3}$$

The maximum value of the right-hand side of Eq. (3) is taken at

$$R = \frac{r^2}{1 + 2\log_4\left(1 - H_4^{-1}\left(\frac{1-r}{2}\right)\right)}$$

and does not vanish for any R, $0 < R < 1$. We summarize the result in the following theorem.

Theorem 2.5. *For any R, $0 < R < 1$, we can construct a family of asymptotically good concatenated quantum codes of rate R and relative minimum distance δ that satisfy Eq. (3).*

Eq. (3) is a quantum analogue of the Zyablov bound for classical concatenated codes [8, Corollary 4.6]. This is the reason why we call Q a quantum Zyablov code.

3 Generalized concatenated quantum codes and the quantum Blokh–Zyablov bound

In this section we present a class of generalized concatenated quantum codes, which is a quantum analogue of classical generalized concatenated codes. For

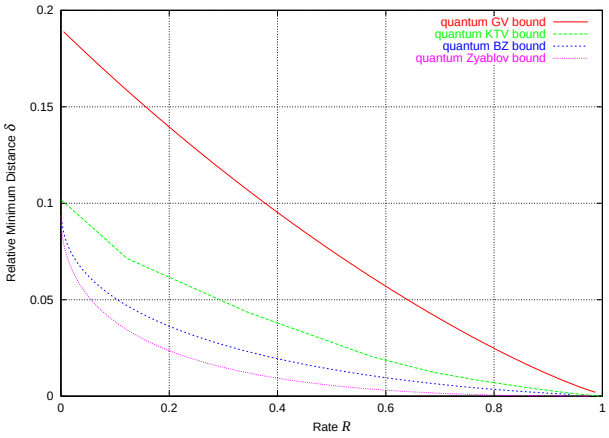

Figure 1: Comparison of the quantum GV, quantum KTV, quantum BZ and quantum Zyablov bounds.

the detail on classical generalized concatenated codes, see [8]. We first give the construction of generalized concatenated quantum codes and then derive minimum distance bounds for generalized concatenated quantum codes. Let s be a positive integer ≥ 2. To construct generalized concatenated quantum codes of order s, we need some notations. Let $Q_1^{(i)}$, $1 \leq i \leq s$, be an $[[mn_1, m(n_1 - 2k_i)]]$ quantum RS code, where m is a positive integer and $n_1 = 2^m - 1$, with associated codes B_i, $B_i^\perp$ with parameters $(mn_1, 2^{mn_1 - m(n_1 - 2k_i)})$, $(mn_1, 2^{mn_1 + m(n_1 - 2k_i)})$, which are obtained from a binary expansion of a dual pair of classical RS codes. Recall that the quantum RS code $Q_1^{(i)}$ has minimum distance at least $k_i + 1$. Furthermore, let $Q_2^{(j)}$, $1 \leq j \leq s$, be an $[[n_2, r_j n_2, \delta_j n_2]]$ quantum code, where $r_j = jm/n_2$, with associated codes C_j, $C_j^\perp$ with parameters $(n_2, 2^{n_2 - jm})$, $(n_2, 2^{n_2 + jm})$ such that $C_s \subseteq C_{s-1} \subseteq \cdots \subseteq C_1$. Consider the direct sums $B = B_1 \oplus B_2 \cdots \oplus B_s$ and $B^\perp = B_1^\perp \oplus B_2^\perp \cdots \oplus B_s^\perp$ (see [3]). Note that the dual of B is $B^\perp$ and that $B \subseteq B^\perp$. We consider each $B_i^\perp$ as a block code over an alphabet of size 4^m, as in the previous section, and write a codeword $\boldsymbol{b}_i$ of $B_i^\perp$ as $\boldsymbol{b}_i = (b_{i,1}, b_{i,2}, \cdots, b_{i,n_1})$, where $b_{i,l} \in \mathbb{F}_4^m$, $1 \leq l \leq n_1$, and we regard $\boldsymbol{b} = (\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_s) \in B^\perp$ as an $s \times n_1$ matrix over $\mathbb{F}_4^m$ whose i-th row is $\boldsymbol{b}_i$.

Let $\mathcal{B}_j$, $1 \leq j \leq s$, be the set of $2m$ vectors of $C_j^\perp$ given in Appendix C. We now give the detail on the construction of a generalized concatenated quantum code of order s. Consider the quotient map $\pi_s : C_s^\perp \to C_s^\perp / C_s$. Since the quotient space $C_s^\perp / C_s$ that has a natural symplectic structure is isomorphic to $\mathbb{F}_4^{sm}$ as a symplectic space, there exists an inner-product-preserving map ρ from $\mathbb{F}_4^{sm}$ to $C_s^\perp / C_s$. We can assume that the j-th block of $\mathbb{F}_4^{sm}$ corresponds to $\mathrm{span}(\pi_s(\mathcal{B}_j))$, where $1 \leq j \leq s$. Using this ρ we map the j-th column $\boldsymbol{c}_j$ of $\boldsymbol{b} \in B^\perp$ above, i.e., $\boldsymbol{c}_j = (b_{1,j}, b_{2,j}, \cdots, b_{s,j}) \in \mathbb{F}_4^{sm}$, to $\rho(\boldsymbol{c}_j) \in C_s^\perp / C_s$ and obtain a map from $B^\perp$ to $\left(C_s^\perp / C_s\right)^{n_1}$, which is also denoted by ρ. As in the previous sec-

tion, from $B \subseteq B^{\perp}$ and ρ we can construct additive codes $C \subseteq C^{\perp}$ with parameters $(n_1 n_2, 2^{n_1 n_2 - \sum_{j=1}^{s} m(n_1 - 2k_j)})$, $(n_1 n_2, 2^{n_1 n_2 + \sum_{j=1}^{s} m(n_1 - 2k_j)})$. The quantum code Q with associated codes $C \subseteq C^{\perp}$ has rate R given by

$$R = r - \frac{2r}{s} \sum_{j=1}^{s} r'_j, \tag{4}$$

where $r = r_s$ and $r'_j = k_j / n_1$.

Lemma 3.1. *Suppose that $\delta_1 \geq \delta_2 \geq \cdots \geq \delta_s$. Let δ be the relative minimum distance of Q. Then*

$$\delta \geq \min_{1 \leq j \leq s} \delta_j r'_j.$$

Proof. Let $\boldsymbol{c} \in C^{\perp} \setminus C$. As in Lemma 2.4, $\boldsymbol{c}$ is written as $\boldsymbol{c} = \rho(\boldsymbol{b}) + \boldsymbol{u}$, where $\boldsymbol{b} = (\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_s)$ is a nonzero vector of $B^{\perp}$ and $\boldsymbol{u} \in C_s^{n_1}$. Suppose that $\boldsymbol{b}_l = \boldsymbol{0}$, $j+1 \leq l \leq s$, and $\boldsymbol{b}_j$ is the last nonzero row of $\boldsymbol{b}$. Since $\boldsymbol{b}_j$ has at least $k_j + 1$ nonzero components and each encoded column of $\boldsymbol{b}$ is in $\pi_s(C_j^{\perp})$, the weight of $\boldsymbol{c} = \rho(\boldsymbol{b}) + \boldsymbol{u}$ is at least $\delta_j n_2 (k_j + 1)$. Since j ranges over the set $\{1, 2, \ldots, s\}$, the minimum weight of $C^{\perp} \setminus C$ is at least $\min_{1 \leq j \leq s} \delta_j n_2 (k_j + 1)$. Hence the minimum distance of Q is at least $\min_{1 \leq j \leq s} \delta_j n_2 (k_j + 1)$ and the statement follows. □

To derive a bound for asymptotically good generalized concatenated quantum codes of order s, we need a sequence of self-orthogonal additive codes C_i, $1 \leq i \leq s$, over $\mathbb{F}_4$ of the same length satisfying the following two conditions:

i) $C_s \subseteq C_{s-1} \subseteq \cdots \subseteq C_1$.

ii) Each quantum code Q_i corresponding to the additive codes $C_i \subseteq C_i^{\perp}$ meets the quantum GV bound (1).

Quantum codes Q_i above have natural inclusion: $Q_1 \subseteq Q_2 \subseteq \cdots \subseteq Q_s$. The following lemma is a quantum version of [8, Lemma 4.10].

Lemma 3.2. *Let $0 < r_1 < r_2 < \cdots < r_s < 1$. For all sufficiently large n, there exist s nested quantum codes Q_i, $1 \leq i \leq s$, with parameters $[[n, r_i n, \delta_i n]]$, which simultaneously meet the quantum GV bound*

$$\delta_i \geq H_4^{-1}\left(\frac{1 - r_i}{2}\right), \quad 1 \leq i \leq s. \tag{5}$$

The proof of Lemma 3.2 is given in Appendix D. The following is a quantum version of [8, Theorem 4.11]:

Theorem 3.3. *For any r, $0 < r < 1$, and $\delta < H_4^{-1}(\frac{1-r}{2})$ we can construct asymptotically good generalized concatenated quantum codes of order s, relative minimum distance at least $\delta/2$ and rate R given by*

$$R = r - \frac{r}{s} \sum_{j=1}^{s} \delta / H_4^{-1}\left(\frac{1}{2}\left(1 - \frac{rj}{s}\right)\right). \tag{6}$$

Proof. We use the notations used in the construction of the generalized concatenated quantum code Q above. Recall that $r_j = jm/n_2$, $1 \leq j \leq s$. We choose the rate r_s of the s-th inner quantum code $Q_2^{(s)}$ satisfying $r_s = r$. Hence $0 < r_1 < r_2 < \cdots < r_s = r$. From Lemma 3.1 the relative minimum distance of Q is at least $\min_{1 \leq j \leq s} \delta_j r'_j$. From Lemma 3.2 we can take $\delta_j = H_4^{-1}(\frac{1-r_j}{2})$. For this value of δ_j we set $r'_j = \frac{\delta}{2H_4^{-1}\left(\frac{1-r_j}{2}\right)}$. Note that $0 < r'_j < 1/2$. Hence the relative minimum distance of Q is at least $\delta/2$ and Eq. (4) gives the rate R of Q. □

Maximizing R with respect to r in Theorem 3.3, we obtain the following:

Corollary 3.4. *For any δ, $0 < \delta < H_4^{-1}(1/2)$, there exist a generalized concatenated quantum code of order s, relative minimum distance at least $\delta/2$ and rate R given by*

$$R = \max_{0<r<1-2H_4(\delta)} r - \frac{r}{s} \sum_{j=1}^{s} \delta / H_4^{-1} \left(\frac{1}{2} \left(1 - \frac{rj}{s} \right) \right). \tag{7}$$

Taking $s \to \infty$ in Theorem 3.3, we obtain the following:

Corollary 3.5. *For any δ, $0 < \delta < H_4^{-1}(1/2)$ and sufficiently large s, there exist a generalized concatenated quantum code of order s, relative minimum distance at least $\delta/2$ and rate close to*

$$R = 1 - 2H_4(\delta) - \delta \int_0^{1-2H_4(\delta)} \frac{dx}{H_4^{-1}\left(\frac{1-x}{2}\right)}. \tag{8}$$

Eq. (8) is a quantum analogue of the Blokh–Zyablov (BZ) bound [8, Corollary 4.13]. We compare the quantum GV bound (1), the quantum Zyablov bound (3) and the quantum BZ bound (8) in Fig. 1.

4 The quantum Katsman–Tsfasman–Vlăduţ bound

In this section we present a class of concatenated quantum codes based on algebraic geometry codes. We use the result of [22]. Let $q = 2^m$, where m is a positive integer. We need the Garcia–Stichtenoth tower of function fields over $\mathbb{F}_{q^2}$.

Definition 4.1 ([12]). Let $F_1 := \mathbb{F}_{q^2}(x_1)$ be the rational function field over $\mathbb{F}_{q^2}$. For $i \geq 1$, we set

$$F_{i+1} := F_i(z_{i+1}),$$

where z_{i+1} satisfies the equation

$$z_{i+1}^q + z_{i+1} = x_i^{q+1},$$

with $x_i = z_i / x_{i-1}$, $i \geq 2$.

Let $n_i = (q^2-1)q^{i-1}$. The zero divisor of $x_1^{q^2-1}-1 \in F_i$ consists of n_i places of degree one and hence we denote it by $P_1 + P_2 + \cdots + P_{n_i}$. For a divisor D of $F_i/\mathbb{F}_{q^2}$ with $\mathrm{supp}D \cap \{P_1, P_2, \cdots, P_{n_i}\} = \emptyset$, we define a linear code $C(D)$ over $\mathbb{F}_{q^2}$ as

$$C(D) = \{(f(P_1), f(P_1), \cdots, f(P_{n_i})) \mid f \in \mathcal{L}(D)\}.$$

Let g_i be the genus of $F_i/\mathbb{F}_{q^2}$. For each i and $0 \le j \le n_i/2 - g_i$, there exists a divisor H of $F_i/\mathbb{F}_{q^2}$ such that the following two conditions hold:

i) $C(H) \subseteq C(H)^\perp$.

ii) $C(H)^\perp$ has dimension $n_i/2 + j$ and minimum distance at least $n_i/2 - g_i + 1 - j$.

For the explicit form of H see [22]. As in the case of quantum RS codes, using the binary expansion of the codes $C(H)$, $C(H)^\perp$ over $\mathbb{F}_{q^2}$ we obtain additive codes C, $C^\perp$ with parameters $(2mn_i, 2^{2mn_i-4mj})$, $(2mn_i, 2^{2mn_i+4mj})$. The quantum code Q_1 with associated codes C, $C^\perp$ has parameters $[[2mn_i, 4mj, d_1 \ge n_i/2 - g_i + 1 - j]]$. The rate r_1 of Q_1 is given by $r_1 = 2j/n_i$. Let Q_2 be a quantum code with parameters $[[n, r_2 n, \delta_2 n]]$, where $r_2 = 2m/n$. The concatenation of Q_1 with Q_2 gives an $[[nn_i, r_1 r_2 n n_i]]$ quantum code with relative minimum distance δ that satisfies

$$\delta \ge \delta_2 \left(\frac{1-r_1}{2} - \frac{g_i}{n_i} \right), \quad 0 \le r_1 \le 1 - \frac{2g_i}{n_i}. \tag{9}$$

Since $\lim_{i\to\infty} \frac{g_i}{n_i} = \frac{1}{q-1}$, taking $i \to \infty$ in (9) leads to

$$\delta \ge \delta_2 \left(\frac{1-r_1}{2} - \frac{1}{q-1} \right), \quad 0 \le r_1 \le \frac{q-3}{q-1}. \tag{10}$$

Setting $R = r_1 r_2$, we obtain

$$\delta \ge \delta_2 \left(\frac{r_2 - R}{2r_2} - \frac{1}{q-1} \right), \quad \frac{q-1}{q-3} R \le r_2 \le 1. \tag{11}$$

Eq. (11) is a quantum analogue of the Katsman–Tsfasman–Vlăduţ (KTV) bound [19]. Since there are many good quantum codes for short block lengths (see [3, Table III]), we can choose a good quantum code Q_2. We optimized the right-hand side of Eq. (11) with respect to Q_2 using the table in [3] and obtained a quantum KTV bound, which is shown in Fig. 1. In Fig. 2 we compare several lower bounds for constructive quantum codes, that is, the quantum KTV bound, the Ashikhmin–Litsyn–Tsfasman–Matsumoto (ALTM) bound [1, 22], the Chen–Ling–Xing (CLX) bound [6], the quantum BZ bound and the quantum Zyablov bound. As can be seen from Fig. 2, the quantum KTV bound is superior to the ALTM bound for rates lower than about 0.5, and the quantum BZ bound and the quantum Zyablov bound are superior to the CLX bound for very low rates. The quantum KTV bound can be improved by using more efficient quantum codes not in the table in [3].

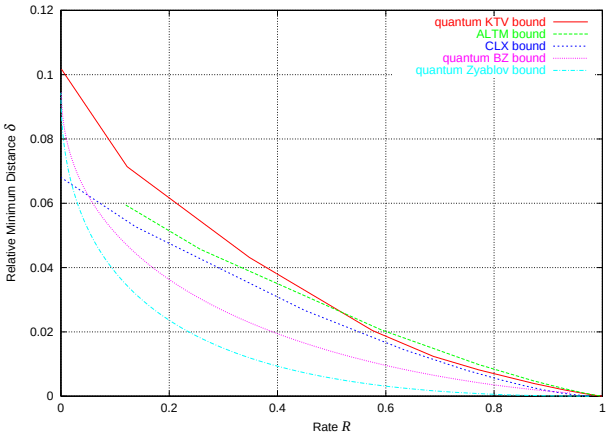

Figure 2: Comparison of the quantum KTV, ALTM, CLX, quantum BZ and quantum Zyablov bounds.

5 Decoding concatenated quantum codes

In this section we give a decoding algorithm for concatenated quantum codes. Let us now consider the quantum Zyablov code Q constructed in Section 2, for example. Q is the concatenation of a quantum RS outer code Q_1 with an inner quantum code Q_2. Suppose that Q_1 has associated codes C_1, $C_1^{\perp}$, and that Q_2 has associated codes C_2, $C_2^{\perp}$. The decoding algorithm consists of the following two steps:

1. *Inner Decoding:* For each inner code Q_2 of Q:
   (a) Measure the generators of C_2 and estimate the most likely errors from the measurement result.
   (b) Correct the errors and decode the encoded data.
2. *Outer Decoding:*
   (a) Correct the remaining errors in the quantum RS outer code Q_1 of Q by using the CSS code structure of Q_1.
   (b) Re-encode each block of Q_1 using Q_2, if necessary.

As in the case of classical concatenated codes [8, Theorem 5.1], it can be proven that the above decoding algorithm can correct up to $\delta N/4$ errors, where δ is the lower bound on the relative minimum distance of Q and N is the overall block length of Q, i.e., the number of qubits of Q. We remark that the estimation of the most likely errors in Q_2 and the computation of the positions and types (bit flip, phase flip, or both) of the errors in Q_2 can be done on a classical computer. The estimation using exhaustive search takes time exponential in

the block length of the inner code, which is $\log N$. Hence for each inner code the estimation complexity is $O(N)$ and the total complexity of estimating the errors in all inner codes is $O(N^2)$. The measurement and correction of all inner codes require $O(N(\log N)^2)$ quantum operations. On the other hand, Q_1 can be decoded in $O(N^2)$ time using the Berlekamp–Massey algorithm on a classical computer. The syndrome computation and correction of Q_1 require $O(N^2)$ quantum operations. Since any classical polynomial time algorithm can be done on a quantum computer in polynomial time, the decoding algorithm above can be implemented on a quantum computer in polynomial time. The above decoding algorithm applies also for concatenated quantum codes based on algebraic geometry codes. As in the case of classical concatenated codes, it is possible to correct up to $\delta N/2$ errors with generalized minimum distance decoding [11, 8].

Finally, we remark the fidelity of the quantum Zyablov code Q above. It is shown in [16] that there exists a sequence of stabilizer quantum codes of rate smaller than some quantity such that the fidelity of a code in the sequence converges to 1 exponentially as the block length grows. Using this result, we can show that if the block length of Q is enough large, then the fidelity of Q is arbitrarily close to 1. The proof is essentially the same as the classical counterpart [8, Theorem 4.15].

6 Conclusion

In this paper we have presented several constructions of asymptotically good concatenated quantum codes. Concatenated quantum codes have simple structure and can be decoded efficiently in polynomial time. Although we focus on the binary concatenated quantum codes, the extension to nonbinary concatenated quantum codes is straightforward.

Acknowledgments

The author would like to thank Prof. H. Yamamoto of the University of Tokyo for support.

References

[1] A. Ashikhmin, S. Litsyn and M. Tsfasman, "Asymtotically good quantum codes," *Phys. Rev. A*, vol. 63, 032311, 2001.

[2] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, "Quantum error correction and orthogonal geometry," *Phys. Rev. Lett*, vol. 78, no. 3, pp. 405–408, 1997.

[3] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Trans. Inform. Theory*, vol. 44, no. 4, pp. 1369–1387, 1998.

[4] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A*, vol. 54, no. 2, pp. 1098–1105, 1996.

[5] H. Chen, "Some good quantum error-correcting codes from algebraic-geometric codes," *IEEE Trans. Inform. Theory*, vol. 47, no. 5, pp. 2059–2061, 2001.

[6] H. Chen, S. Ling and C. Xing, "Asymptotically good quantum codes exceeding the Ashikhmin-Litsyn-Tsfasman bound," *IEEE Trans. Inform. Theory*, vol. 47, no. 5, pp. 2055–2058, 2001.

[7] H. Chen, S. Ling and C. Xing, "Quantum codes from concatenated algebraic-geometric codes," *IEEE Trans. Inform. Theory*, vol. 51, no. 8, pp. 2915–2920, 2005.

[8] I. I. Dumer, "Concatenated codes and their multilevel generalizations," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman (Ed.), Elsevier Science, 1998.

[9] A. Ekert and C. Macchiavello, "Quantum error correction for communication," *Phys. Rev. Lett*, vol. 77, no. 12, pp. 2585–2588, 1996.

[10] G. D. Forney, *Concatenated Codes*, Cambridge, MA: MIT Press, 1966.

[11] G. D. Forney, "Generalized minimum distance decoding," *IEEE Trans. Inform. Theory*, vol. 12, no. 2, pp. 125–131, 1966.

[12] A. Garcia and H. Stichtenoth, "A tower of Artin–Schreier extensions of function fields attaining the Drinfeld–Vladut bound," *Invent. Math.*, vol. 121, no. 1, pp. 211–222, 1995.

[13] D. Gottesman, "Class of quantum error-correcting codes saturating the quantum Hamming bound," *Phys. Rev. A*, vol. 54, pp. 1862–1868, 1996.

[14] D. Gottesman, *Stabilizer Codes and Quantum Error Correction*, Ph.D. Thesis, California Institute of Technology, Pasadena, CA, 1997.

[15] M. Grassl, W. Geiselmann and T. Beth, "Quantum Reed-Solomon codes," AAECC-13, LNCS 1709, pp. 231–244, 1999.

[16] M. Hamada, "Lower bounds on the quantum capacity and highest error exponent of general memoryless channels," *IEEE Trans. Inform. Theory*, vol. 48, no. 9, pp. 2547–2557, 2002.

[17] M. Hamada, "Information rates achievable with algebraic codes on quantum discrete memoryless channels," *IEEE Trans. Inform. Theory*, vol. 51, no. 12, pp. 4263–4277, 2005.

[18] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, 2003.

[19] G. L. Katsman, M. A. Tsfasman and S. G. Vlăduţ, "Modular curves and codes with a polynomial construction," *IEEE Trans. Inform. Theory*, vol. 30, no. 2, pp. 353–355, 1984.

[20] E. Knill and R. Laflamme, "Concatenated quantum codes," LANL e-print quant-ph/960812.

[21] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

[22] R. Matsumoto, "Improvement of Ashikhmin-Litsyn-Tsfasman bound for quantum codes," *IEEE Trans. Inform. Theory*, vol. 48, no. 7, pp. 2122–2124, 2002.

[23] E. M. Rains, "Quantum weight enumerators," *IEEE Trans. Inform. Theory*, vol. 44, no. 4, pp. 1388–1394, 1998.

[24] A. M. Steane, "Multiple particle interference and quantum error correction," *Proc. Roy. Soc. Lond. A*, vol. 452, pp. 2551–2557, 1996.

[25] V. V. Zyablov, "An estimate of the complexity of constructing binary linear cascade codes," *Probl. Inform. Transm.*, vol. 7, no. 1, pp. 3–10, 1971.

Appendix

A Proof of Theorem 2.1

Following the argument in [4, Sect. V], we prove Theorem 2.1. Counting arguments used in the proofs below can also be found in [18, Sect. 9.5] and [21, Sect. 7 in Chap. 17, Sect. 6 in Chap. 19].

Lemma A.1. *Let $\boldsymbol{v}$ be a nonzero vector of $\mathbb{F}_4^n$ and C self-orthogonal additive code over $\mathbb{F}_4$ of length n and dimension $k+1$ containing $\boldsymbol{v}$. Then C contains 2^k-1 self-orthogonal additive subcodes of dimension k containing $\boldsymbol{v}$.*

Proof. We first remark that a subcode of C is obviously self-orthogonal. Let $C_0 := \{\mathbf{0}, \boldsymbol{v}\}$. Then C_0 is a one dimensional additive subcode. Consider the quotient map $C \to C/C_0$. Note that C/C_0 is a k-dimensional binary vector space. Let S be the set of k-dimensional subcodes of C containing $\boldsymbol{v}$. Then S is identified with the set of $(k-1)$-dimensional subspaces of C/C_0. The total number of $(k-1)$-dimensional subspaces of C/C_0 is 2^k-1, which completes the proof. □

Lemma A.2. *Let $\boldsymbol{v}$ be a nonzero vector of $\mathbb{F}_4^n$, and for $1 \le k \le n$, let σ_k be the number of self-orthogonal additive codes of length n over $\mathbb{F}_4$ and dimension k containing $\boldsymbol{v}$. Then*

$$\sigma_k = \prod_{i=1}^{k-1} \frac{2^{2(n-i)}-1}{2^i-1}$$

Proof. It is obvious that $\sigma_1 = 1$, since a self-orthogonal additive code of length n over $\mathbb{F}_4$ and dimension 1 containing $\boldsymbol{v}$ is only $C_0 := \{\mathbf{0}, \boldsymbol{v}\}$. Let C be a self-orthogonal additive code over $\mathbb{F}_4$ of length n and dimension k containing $\boldsymbol{v}$, and let S be the set of self-orthogonal additive code over $\mathbb{F}_4$ of length n and dimension $k+1$ containing C. If $C' \in S$, then $C \subseteq C' \subseteq C'^{\perp} \subseteq C^{\perp}$. Consider the quotient map $C^{\perp} \to C^{\perp}/C$. Then S is identified with the set of $2^{2(n-k)}-1$ cosets of C in $C^{\perp}$, i.e., all the cosets other than C. Let $C' \in S$. By Lemma A.1, C' contains 2^k-1 self-orthogonal additive subcodes of dimension k containing $\boldsymbol{v}$. Therefore we have

$$\sigma_{k+1} = \frac{2^{2(n-k)}-1}{2^k-1}\sigma_k.$$

Using this recursion we obtain the expression for σ_k as in the statement. □

Lemma A.3. *Let $\boldsymbol{v}$ be a nonzero vector of $\mathbb{F}_4^n$, and for $1 \le k \le n-1$, let τ_k be the number of self-orthogonal additive codes C over $\mathbb{F}_4$ of length n and dimension k satisfying $\boldsymbol{v} \in C^{\perp} \setminus C$. Then*

$$\tau_k = 2^k \prod_{i=1}^{k} \frac{2^{2(n-i)}-1}{2^i-1}$$

Proof. Let S be the set of self-orthogonal additive codes C over $\mathbb{F}_4$ of length n and dimension k satisfying $\boldsymbol{v} \in C^\perp \setminus C$. Then τ_k is the cardinality of the set S. Pick $C \in S$ and consider the code C' generated by C and $\boldsymbol{v}$. Then C' is an self-orthogonal additive code of dimension $k+1$ containing $\boldsymbol{v}$. C' contains $2^{k+1}-1$ subcodes of dimension k, and from Lemma A.1, 2^k-1 of these subcodes contain $\boldsymbol{v}$. Hence C' contains 2^k subcodes of dimension k not containing $\boldsymbol{v}$. By Lemma A.2 the number of self-orthogonal additive code of dimension $k+1$ containing $\boldsymbol{v}$ is σ_{k+1}. Hence we have $\tau_k = 2^k \sigma_{k+1}$. □

We are now ready to prove Theorem 2.1. Let Φ be the set of all self-orthogonal additive codes over $\mathbb{F}_4$ of length n and dimension $n-k$, and let $\Phi^\perp := \{C^\perp \mid C \in \Phi\}$. From Lemmas A.2 and A.3, each nonzero vector $\boldsymbol{v} \in \mathbb{F}_4^n$ belongs to the same number N of codes in $\Phi^\perp$, where $N = \sigma_{n-k} + \tau_{n-k}$. Hence we have

$$N\left(2^{2n}-1\right) = |\Phi^\perp|\left(2^{n+k}-1\right).$$

If $N\sum_{i=1}^{d-1} 3^i \binom{n}{i} < |\Phi^\perp|$, i.e.,

$$\sum_{i=1}^{d-1} 3^i \binom{n}{i} < \frac{2^{2n}-1}{2^{n+k}-1}, \tag{12}$$

then there exists an additive code $C^\perp \in \Phi^\perp$ that has minimum distance $\geq d$.

B The symplectic structure of $C_2^\perp/C_2$

Since $C_2^\perp \subseteq \mathbb{F}_4^{n_2}$ and $\mathbb{F}_4^{n_2}$ has the symplectic inner product $\langle \cdot, \cdot \rangle$ defined in Section 2, we define a symplectic inner product on $C_2^\perp/C_2$ as

$$\langle \boldsymbol{u} + C_2, \boldsymbol{v} + C_2 \rangle := \langle \boldsymbol{u}, \boldsymbol{v} \rangle,$$

where $\boldsymbol{u}, \boldsymbol{v} \in C_2^\perp$. It is easy to see that this definition does not depend on representatives $\boldsymbol{u}, \boldsymbol{v}$, and that the induced form on $C_2^\perp/C_2$ is nondegenerate.

Let $\{b_1, b_2, \ldots, b_m\}$ be the standard basis of $\mathbb{F}_4^m$, i.e., $b_i = (\delta_{ij})_j$, where δ_{ij} is the Kronecker delta. We set

$$e_i = \omega b_i, \quad f_i = \bar{\omega} b_i, \quad 1 \leq i \leq m.$$

Then

$$\langle e_i, f_j \rangle = \delta_{ij}, \quad \langle e_i, e_j \rangle = 0, \quad \langle f_i, f_j \rangle = 0.$$

It follows from the following lemma that there exists an inner-product-preserving map from $\mathbb{F}_4^m$ to $C_2^\perp/C_2$.

Lemma B.1. *For any $2m$-dimensional binary vector space V with nondegenerate symplectic form $(\cdot, \cdot)$, there exists a basis $\{g_i, h_i, 1 \leq i \leq m\}$ of V over $\mathbb{F}_2$ such that*

$$(g_i, h_j) = \delta_{ij}, \quad (g_i, g_j) = 0, \quad (h_i, h_j) = 0.$$

Proof. We show the statement by induction on m. In the case $m = 1$, pick a nonzero vector $v \in V$. Since the form $(\cdot, \cdot)$ is nondegenerate, there exists another vector $v' \in V$ that satisfies $(v, v') = 1$. $g_1 = v$ and $h_1 = v'$ give a desired basis.

Suppose that the statement holds for any $2(m-1)$-dimensional binary vector space with a nondegenerate symplectic form. Let V be a $2m$-dimensional binary vector space with nondegenerate symplectic form $(\cdot, \cdot)$. As explained above, we can take vectors $g_1, h_1 \in V$ that satisfies $(g_1, h_1) = 1$. Let $W = \mathrm{span}\{g_1, h_1\}$ and consider the space $W^\perp$. Since the form $(\cdot, \cdot)$ is nondegenerate, the dimension of $W^\perp$ is $2(m-1)$. It is easy to see that $W \cap W^\perp = \{0\}$. Hence V is the direct sum of W and $W^\perp$, and the restriction of $(\cdot, \cdot)$ to $W^\perp$ gives a nondegenerate symplectic form on $W^\perp$. By hypothesis there exist a basis $\{g_i, h_i, 2 \le i \le m\}$ of $W^\perp$ over $\mathbb{F}_2$ such that

$$(g_i, h_j) = \delta_{ij}, \quad (g_i, g_j) = 0, \quad (h_i, h_j) = 0.$$

Hence the set $\{g_i, h_i, 1 \le i \le m\}$ gives a desired basis. □

C The set $\mathcal{B}_j$

We first remark that $C_s \subseteq C_{s-1} \subseteq \cdots C_1 \subseteq C_1^\perp \subseteq C_2^\perp \subseteq \cdots \subseteq C_s^\perp$. Consider the quotient map $\pi_1 : C_1^\perp \to C_1^\perp / C_1$. We can take a basis $\{\bar{g}_i, \bar{h}_i, 1 \le i \le m\}$ of $C_1^\perp / C_1$ over $\mathbb{F}_2$ such that

$$\langle \bar{g}_i, \bar{h}_j \rangle = \delta_{ij}, \quad \langle \bar{g}_i, \bar{g}_j \rangle = 0, \quad \langle \bar{h}_i, \bar{h}_j \rangle = 0. \tag{13}$$

We choose $g_i, h_i \in C_1^\perp$, $1 \le i \le m$, that satisfy $\pi_1(g_i) = \bar{g}_i$ and $\pi_1(h_i) = \bar{h}_i$. The following is easily checked:

$$\langle g_i, h_j \rangle = \delta_{ij}, \quad \langle g_i, g_j \rangle = 0, \quad \langle h_i, h_j \rangle = 0. \tag{14}$$

From Eq. (14), it follows that $\mathcal{B}_1 = \{g_i, h_i, 1 \le i \le m\}$ are linearly independent, and that C_1 and $\mathcal{B}_1$ span $C_1^\perp$.

Next, consider the quotient map $\pi_2 : C_2^\perp \to C_2^\perp / C_2$. Let $\bar{g}_i = \pi_2(g_i)$, $\bar{h}_i = \pi_2(h_i)$, $1 \le i \le m$. Although we use the same notation above, $\bar{g}_i$ and $\bar{h}_i$ here are elements of $C_2^\perp / C_2$. Note that for $\bar{g}_i$, $\bar{h}_i$, $1 \le i \le m$, the same equations as in Eq. (13) with a natural symplectic form on $C_2^\perp / C_2$ are satisfied. We can take $\bar{g}_i$, $\bar{h}_i$, $m+1 \le i \le 2m$, of $C_2^\perp / C_2$ in such a way that the same equations as in Eq. (13) with $1 \le i, j \le 2m$ are satisfied. We choose $g_i, h_i \in C_2^\perp$, $m+1 \le i \le 2m$, that satisfy $\pi_2(g_i) = \bar{g}_i$ and $\pi_2(h_i) = \bar{h}_i$. It is easily checked that the same equations as in Eq. (14) with $1 \le i, j \le 2m$ are satisfied. As in the case of $C_1^\perp$, it is also easily checked that $\mathcal{B}_2 = \{g_i, h_i, 1 \le i \le 2m\}$ are linearly independent, and that C_2 and $\mathcal{B}_2$ span $C_2^\perp$. We inductively define $\mathcal{B}_i$, $i \ge 3$, and obtain $\mathcal{B}_s = \{g_i, h_i, 1 \le i \le sm\}$ that satisfy the same equations as in Eq. (14) with $1 \le i, j \le sm$. Note that the vectors in $\mathcal{B}_i$ are linearly independent, and that C_i and $\mathcal{B}_i$ span $C_i^\perp$.

We redefine $\mathcal{B}_j$, $1 \le j \le s$, as $\mathcal{B}_j = \{g_i, h_i, (j-1)m + 1 \le i \le jm\}$ ($\mathcal{B}_1$ is the same as above).

D Proof of Lemma 3.2

We prove the case $s = 2$ only. The general case is a straightforward extension of the case $s = 2$. Let $0 \le r_1 \le r_2 \le 1$ and sufficiently large n be given. Without loss of generality, we may assume that $k_i = r_i n$, $i = 1, 2$, are positive integers. Let C_1 be a self-orthogonal additive code over $\mathbb{F}_4$ with parameters $(n, 2^{n-k_1})$ and suppose that its dual $C_1^\perp$ has minimum distance $d_1 = \delta_1 n$, where $\delta_1 = H_4^{-1}\left(\frac{1-r_1}{2}\right)$. This is possible from Theorem 2.1. We need to show that there exists a self-orthogonal additive code C_2 over $\mathbb{F}_4$ with parameters $(n, 2^{n-k_2})$ such that the following two conditions hold:

i) $C_2 \subseteq C_1$.

ii) The dual $C_2^\perp$ of C_2 has minimum distance $d_2 = \delta_2 n$, where $\delta_2 = H_4^{-1}\left(\frac{1-r_2}{2}\right)$.

Consider the quotient map $\pi : \mathbb{F}_4^n \to \mathbb{F}_4^n / C_1^\perp$. Note that the quotient space $\mathbb{F}_4^n / C_1^\perp$ is a $(n - k_1)$-dimensional binary vector space. We define the weight of a coset to be the smallest weight of a vector in the coset, i.e., the weight of a coset is the weight of a coset leader. Let $\Psi_{k_2-k_1}$ be the set of $(k_2 - k_1)$-dimensional subcodes of $\mathbb{F}_4^n / C_1^\perp$. If $C \in \Psi_{k_2-k_1}$, then $\widetilde{C} := \pi^{-1}(C)$ is an $(n + k_2)$-dimensional additive code over $\mathbb{F}_4$ containing $C_1^\perp$. Let $d := \mathrm{dist}(C)$. Then it is easy to see that $\mathrm{dist}(\widetilde{C}) = \min\{d, d_1\}$. (Consider the decomposition $\widetilde{C} = \cup_{\boldsymbol{v} \in \pi^{-1}(C)} \boldsymbol{v} + C_1^\perp$.) Let S be the set of cosets of nonzero weight smaller than d. Since S is in the image of the set of nonzero vectors of $\mathbb{F}_4^n$ of weight smaller than d under π, we have

$$|S| \le \sum_{i=1}^{d-1} 3^i \binom{n}{i}.$$

As in the proof of Theorem 2.1, we can prove that for $\boldsymbol{v} \notin C_1^\perp$, the number of codes in $\Psi_{k_2-k_1}$ containing $\boldsymbol{v} + C_1^\perp$ is independent of $\boldsymbol{v} + C_1^\perp$. We denote the number by N. Hence we have

$$N(2^{n-k_1} - 1) = |\Psi_{k_2-k_1}|(2^{k_2-k_1} - 1).$$

If $N|S| \le N \sum_{i=1}^{d-1} 3^i \binom{n}{i} < |\Psi_{k_2-k_1}|$, i.e.,

$$\sum_{i=1}^{d-1} 3^i \binom{n}{i} < \frac{2^{n-k_1} - 1}{2^{k_2-k_1} - 1}, \tag{15}$$

then there exists an additive code $C \in \Psi_{k_2-k_1}$ that has minimum distance $\ge d$. A standard argument shows that we can take d to be $d_2 = \delta_2 n$. Since $\delta_1 \ge \delta_2$, the corresponding $\widetilde{C}$ has minimum distance d_2. We define $C_2 := \widetilde{C}^\perp$. So $C_2^\perp = \widetilde{C}$ has minimum distance d_2. Since $C_2 \subseteq C_1 \subseteq C_1^\perp \subseteq C_2^\perp$, C_2 is self-orthogonal. Hence the lemma has been proved.